Country	Institution	Module Description	ECTS
GR	**HAFA**	**Social Media Security: Tools & Cases**	**2.0**

	Minimum Qualification for Lecturers
Service **AF**	o English: Common European Framework of Reference for Languages (CEFR) Level B2 or NATO STANAG Level 3.
Language **English**	o Thorough knowledge in Social Networking Platforms o Adequate knowledge in Social Network Analysis Tools o Thorough knowledge of Privacy and Moral Issues

Prerequisites for international participants:	**Goal of the Module**
• English: Common European Framework of Reference for Languages (CEFR) Level B1 or NATO STANAG Level 2. • At least 1 year of national (military) higher education.	• To present the most common social objects and the respective electronic social networking platforms • To familiarize students with various types of sensitive personal data and associated risks and impact of misuse of the social objects • To discuss the most common techniques that are used in social network analysis • To understand the impact of using Artificial Intelligence in producing fake social objects

Learning outcomes		
	Know-ledge	• Knows the personal and organizational risks associated with the use of social networking platforms • Describes and understands the legal implications for those who use the social networking platforms in order to launch threats or try to harm other natural or legal persons, entity or organizations, but also misuse social networking platforms either unwittingly or on purpose • Knows what fake social objects are and how to detect them • Knows the tools that can be used in order to get the best possible protection for social networking risks or threats
	Skills	• Is able to consider the risks of providing personal or work-related information on social networking platforms • Is able to consider the risks of sharing data in public • Is able to understand and protect the right of freedom of expression, but also accept the limitations and respect his/her duties and legal obligations deriving by the laws of the organization he/she serves • Is able to understand issues of responsibility/accountability and liability related to the use or misuse of social media • Is able to understand when it is crucial to report social media misuse and how to report it • Is able to use technology and laws to protect the organization and him/herself
	Responsibility & Autonomy	• Understands the risks of social media exposure and the relative implications • Understands the future security and privacy challenges related to the use of social media

		- Uses the appropriate tools to protect the social identity and discover the actors behind social media attacks - Analyses the information posted in social media and understands the reliability of the source

Verification of Learning Outcomes

Test	• A short exam will be given to the cadets for verifying their understanding of the course topics
Assignment	• An individual assignment will be given to analyse a small social network and study its structure and attributes
Case study	• A case study will be discussed regarding a contemporary social media incident

Module Details

Main Topic	Recom-mended WH	Details
E-learning	4	• Familiarization with the most popular social media platforms • Facebook, LinkedIn, Instagram, Twitter, TikTok, PInterest, Snapchat
Social Media Fundamentals	3	• What are social media • Types of social media and specific risks related to their use • Individual and group identity and freedom vs terms and conditions for getting access to and use the platform
Risks of Social Media	3	• Exposure, Over-exposure and Misuse in the Social Media • Misuse of Personal Information, Photos, Videos • Sharing Health and Fitness Data • Behaviors and Profiling of Individuals and Groups
Attacking an Unsuspected User	4	• Bot or Human Attacks • Account Takeover Attacks • Fraudulent Account Creation Attacks • Spamming • Cyberbullying and Abusing • Social Engineering
Privacy & Security Issues	4	• Privacy Issues • Security Issues • Legal Issues • Ethical Issues • General Data Protection Regulation (GDPR)
Social Network Analysis Tools	5	• Social Networks Analysis Techniques and Tools • Social Engineering Tools • Using Artificial Intelligence in Social Profiling • Deepfake Tools • Visualization Tools
Cases analysis	4	• Deepfakes: Salvador Dalí alive, Bill Hader case, President Obama Speech • Social Media Surveillance: The Strava app case, the Polar Watches case, Driving a Connected Car
Reducing the risks of over-exposure and misuse	2	• Education: Promoting knowledge, providing awareness • Technology: Providing the Tools to detect and prevent Social Media misuse, but also to reveal the truth, if and when needed • Laws: Supplementing the legal background to deter future perpetrators and to provide better protection for the victims
Test	1	• Module examination

Self-Study Hours

Self-Study	20	• The self-study hours are required for the preparation of the daily lectures and for the individual assignment • Extra hours are required for the preparation and contribution at the case study of the course
Total WH	**50**	

Draft: I. Lekea, P. Karampelas .... 06th Jan 2021
Revised by Name(s) Surname(s) XXXXXX
Approved by the Project Committee XXXXXX

List of Abbreviations:

CEFR ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯ Common European Framework of Reference for Languages

ECTS ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯ European Credit Transfer and Accumulation System

NATO ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯ North Atlantic Treaty Organisation

STANAG ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯ Standardization Agreement

WH ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯ Working Hour

GDPR ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯ General Data Protection Regulation

International Air Force Semester
2020-1-EL01-KA203-079068

Co-funded by the Erasmus+ Programme of the European Union